NAME

rapath − print traceroute path information from **argus(8)** data.

COPYRIGHT

SYNOPSIS

rapath [**−A**] [**raoptions**]

DESCRIPTION

Rapath reads **argus** data from an *argus-data* source, and generates the path information that can be formulated from flows that experience ICMP responses. When a packet stimulates the creation of an ICMP response, for whatever reason, the intermediate node that generates the ICMP packet is, by definition, on the path. Argus data perserves this intermediate node address, and **rapath** uses this information to generate path information, for arbitrary IP network traffic. **Rapath** is principally designed to recover traceroute.1 traffic, so that if a trace is done in the network, argus will pick it up and record the intermediate nodes and the RTT for the volleys. However the method is generalized such that it also picks up routing loop conditions, when they exist in the observed packet stream.

Rapath will generate argus flow records that have the src address, dst address and src ttl of the transmitted packet, aggregated so that the average duration, standard deviation, max and min rtt's are preserved. The most accurate estimate of the actual Round-Trip Time (RTT) between a src IP address and an ICMP based intermediate node is the MinDur field. As the number of samples gets larger, the MinDur field approaches the theoretical best case minimum RTT. RTT's above this value, will include variations in network and device delay.

When used in conjunciton with racluster, path information to and from CIDR based network addresses can be calculated, so that traces to multiple machines in the same subnet can be grouped together.

The output of rapath can be piped into ranonymize.1, in order to share path performance information without divulging the actual addresses of intermidate routers.

OPTIONS

Rapath, like all ra based clients, supports a number of **ra options** including filtering of input argus records through a terminating filter expression. See **ra(1)** for a complete description of **ra options**. **rapath(1)** specific options are:

−A Draw a description of the path with a legend.

INVOCATION

A sample invocation of **rapath(1)**. This call reads **argus(8)** data from **inputfile** and generates any path information, based on src and dst IP addresses, and writes the results to stdout. Notice that even with only 12 samples, the MinDur field is in sorted order, where as the Mean and MaxDur do not reflect sorted values.

rapath -r /tmp/ra.out - icmpmap and src ttl lt 20

SrcAddr	Dir	DstAddr	Inode	sTtl	AvgDur	StdDev	MaxDur	MinDur	Trans
207.237.36.98	->	134.207.10.73	10.22.32.1	1	0.007793	0.004256	0.015120	0.004814	12
207.237.36.98	->	134.207.10.73	208.59.246.1	2	0.008504	0.003251	0.015473	0.005943	12
207.237.36.98	->	134.207.10.73	207.172.19.110	3	0.008016	0.002446	0.015037	0.006243	12
207.237.36.98	->	134.207.10.73	4.78.132.5	4	0.009951	0.004558	0.022182	0.006406	12
207.237.36.98	->	134.207.10.73	4.68.16.75	5	0.013511	0.015643	0.062595	0.006955	12
207.237.36.98	->	134.207.10.73	4.68.110.234	6	0.008881	0.002118	0.012951	0.007014	6
207.237.36.98	->	134.207.10.73	204.255.173.53	6	0.010842	0.004799	0.018135	0.007110	6
207.237.36.98	->	134.207.10.73	152.63.3.109	7	0.008853	0.001638	0.011440	0.007382	5

```
207.237.36.98  ->  134.207.10.73   152.63.3.165   7  0.008455  0.000889  0.010081  0.007496   7
207.237.36.98  ->  134.207.10.73   152.63.25.38   8  0.015877  0.002696  0.023995  0.013639  12
207.237.36.98  ->  134.207.10.73   152.63.39.173  9  0.015761  0.002123  0.022057  0.013715  12
207.237.36.98  ->  134.207.10.73   157.130.49.2  10  0.022892  0.021648  0.090687  0.014434  12
207.237.36.98  ->  134.207.10.73    138.18.1.7   11  0.018387  0.001137  0.021117  0.017082  12
207.237.36.98  ->  134.207.10.73   138.18.23.36  12  0.020205  0.002439  0.025719  0.017894  12
207.237.36.98  ->  134.207.10.73   138.18.23.35  13  0.019117  0.000912  0.020662  0.017673  12
```

This sample invocation of **rapath(1)** prints out a graph of the path, suppressing the output of the actual node information (-q).

rapath -qA -r /tmp/ra.out - icmpmap and src ttl lt 20

A -> B -> C -> D -> E -> [F,G] -> [H,I] -> J -> K -> L -> M -> N -> O

SEE ALSO

ra(1), rarc(5), argus(8),

FILES

AUTHORS

Carter Bullard (carter@qosient.com).

BUGS